VA Data Theft - What You Need to Know

(Monday, 05 June 2006) - Contributed by 1Lt. Jeff Roberson - Last Updated ()

From Military.com, dated June 05, 2006

Check out our Identity Theft page for
more articles related to this issue

Topic A – WHAT HAPPENED AND HOW DOES THIS AFFECT ME?

A1. What happened?

The Department of Veterans Affairs (VA) has recently learned that an employee, a data analyst, took home electronic data from VA that was stored in his home on a laptop computer and external hard drive. He was not authorized to take this data home. This behavior was in violation of VA policies.

The employee’s home was burglarized and the computer equipment, along with various other items, was stolen. The electronic data stored on this computer included identifying information for millions of veterans. Authorities believe the computer equipment, rather than any data on it, was the target of the theft. It is possible the perpetrators remain unaware of the information that they possess or of how to make use of it. However, out of an abundance of caution, VA is taking all possible steps to protect and inform our veterans.

A1.a. What action has been taken against this employee or his supervisor?

The employee is cooperating fully with the investigation. The employee was initially placed on administrative leave, and VA is implementing procedures necessary to dismiss the employee. Also, the official responsible for the organization in which this employee served has resigned his position because of the events.

A2. What information was included?

The data lost is primarily limited to an individual’s name, date of birth, and social security number. In some cases, spousal information may have been included. However, this information alone may be useful to identity thieves, and we recommend that all veterans be extra vigilant in monitoring for signs of potential identity theft or misuse of this information. Importantly, the affected data did not include any of VA’s electronic health records or any financial information.

A2.a. I heard on the news that the information stolen included disability ratings. What information does that include?

The information stolen did not include medical information about any veteran,

nor did it include any information from VA’s electronic health records. For some veterans who have applied for VA disability compensation benefits and have been determined by VA to have a disability related to their military service, the data may have included the number of service-connected disabilities a veteran has and the veteran’s overall disability percentage rating.

A3. How do I know if information about me was stolen?

At this point, we do not have information available to confirm the specific veterans whose personal information may have been included in this data loss. An investigation is ongoing. We do not want any veteran to be surprised and are operating under the assumption that some information for all veterans was included. We are informing people of this incident and the possibility that it could involve information about them.

A3a. Does this only affect veterans discharged after 1975?

It potentially affects all living veterans who were discharged after 1975, which is when VA automated its records systems and began regular input of information received from the Department of Defense on all separating veterans.

When VA automated its records systems, VA also input data from all historical claimant records that had been manually maintained by the agency. This data loss therefore also potentially affects all veterans who have ever filed a claim for VA disability compensation, pension, or education benefits, or who have (or had) a VA insurance policy – no matter when the claim was filed or when they were discharged. These veterans would be included even if their claim was denied or they are not currently receiving benefits.

We urge all veterans to be extra vigilant and monitor their financial accounts.

A4. I have never applied for benefits from VA. Do I need to be concerned?

The electronic data on the stolen computer equipment includes information from many veterans who have never filed for VA benefits or contacted VA. Since the 1970s, VA has received information from the Department of Defense on all who served. If you are a veteran, you are encouraged to take steps to protect yourself against identity theft, whether or not you have ever applied for VA benefits.

A5. I am the spouse, widow, or child of a veteran. Was my information included?

It is unclear whether any spousal or dependents’ information has been compromised. However, if this did occur, it appears it would be a very small number of people.

A6. Will I still get my monthly benefit payment?

Yes. There will be no impact on benefit payments.

Topic B – WHAT SHOULD I DO?

B1. What should I do to protect myself? Do I have to close my bank account or cancel my credit cards?

At this point there is no evidence that any missing data has been used illegally. However, the Department of Veterans Affairs is asking all veterans to be extra vigilant and to carefully monitor bank statements, credit card statements and any statements relating to recent financial transactions, and to immediately report any suspicious or unusual activity.

For tips on how to guard against misuse of personal information, visit the Federal Trade Commission website.

You do not have to close your bank account or cancel your credit cards. You should however take steps to protect yourself against identity theft.

One way to monitor your financial accounts is to review your credit report. By law you are entitled to one free credit report each year. Request a free credit report from one of the three major credit bureaus -- Equifax, Experian, TransUnion – at www.AnnualCreditReport.com or by calling 1-877-322-8228.

B1.a. What do you mean by suspicious activity?

Suspicious activities could include the following:

* Inquiries from companies you haven’t contacted or done business with

* Purchases or charges on your accounts you didn’t make

* New accounts you didn’t open or changes to existing accounts you didn’t make

* Bills that don’t arrive as expected

* Unexpected credit cards or account statements

* Denials of credit for no apparent reason

* Calls or letters about purchases you didn’t make

B2. What is identity theft?

Identity theft occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes.

B3. I haven’t noticed any suspicious activity in my financial statements, but what can I do to protect myself and prevent being victimized by credit card fraud or identity theft?

The Department of Veterans Affairs strongly recommends that veterans closely monitor their financial statements and visit the Department of Veterans Affairs special website.

B4. Should I reach out to my financial institutions or will the Department of Veterans Affairs do this for me?

The Department of Veterans Affairs does not believe that it is necessary to contact financial institutions or cancel credit cards and bank accounts, unless you detect suspicious activity.

B5. What is the earliest date at which suspicious activity might have occurred due to this data breach?

The VA employee’s home was burglarized and the computer equipment was stolen on May 3, 2006. If the data has been misused or otherwise used to commit fraud or identity theft crimes, it is likely that veterans may notice suspicious activity during the month of May.

B6. What should I do if I detect a problem with any of my accounts?

The Federal Trade Commission recommends the following four steps if you detect suspicious activity:

Step 1 – Contact the fraud department of one of the three major credit bureaus:

* Equifax: 1-800-525-6285; www.equifax.com;

P.O. Box 740241, Atlanta, GA 30374-0241

* Experian: 1-888-EXPERIAN (397-3742); www.experian.com;

P.O. Box 9532, Allen, Texas 75013

* TransUnion: 1-800-680-7289; www.transunion.com;

Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Step 2 – Close any accounts that have been tampered with or opened fraudulently.

Step 3 – File a police report with your local police or the police in the community where the identity theft took place.

Step 4 – File a complaint with the Federal Trade Commission by using the FTC’s Identity Theft Hotline:

* By telephone 1-877-438-4338

* Online at www.consumer.gov/idtheft

* By mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington DC 20580.

B7. Where can I get more information?

The Department of Veterans Affairs has set up a special website for veterans which features up-to-date news and information.

B8. What are my remedies if my identity is stolen and used illegally?

VA is working aggressively to determine what additional protections we may be able to provide to veterans as a result of this incident. We have not been advised of any special restitution that might be available for any losses related to this specific incident.

The Federal Trade Commission (FTC) has produced a booklet to help you remedy the effects of an identity theft. It describes what steps to take, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The contents of the booklet, Taking Charge: Fighting Back Against Identity Theft, are available on-line.

B9. Can Social Security can put a flag on my number?

No, unlike the credit bureaus, the Social Security Administration cannot put a flag or security alert of any type on your Social Security number.

To report that someone is using your Social Security number, file a complaint with the Federal Trade Commission by using the four steps outlined above:

* Internet— www.consumer.gov/idtheft
* Telephone— 1-877-IDTHEFT (1-877-438-4338)

B10. Can I get a new Social Security number?

The Social Security Administration will not issue you a new Social Security number as a precaution if you are concerned or think your number may have been stolen as part of the VA data theft.

Topic C – WHAT IS VA DOING ABOUT THE SITUATION?

C1. What is VA doing about this?

The Department of Veterans Affairs is working with the President’s Identity Theft Task Force, the Department of Justice and the Federal Trade Commission to investigate this data breach and to develop safeguards against similar incidents. Task Force members have already taken actions to protect the affected veterans, including working with the credit bureaus to help ensure that veterans receive the free credit report they are entitled to under the law.

Appropriate law enforcement agencies, including the Federal Bureau of Investigation (FBI) and the Office of Inspector General of the Department of Veterans Affairs (VA OIG), have launched full-scale investigations into this matter.

C1a. Is a reward being offered?

On May 25, 2006, the VA’s Office of Inspector General (VA OIG) and the FBI announced a $50,000 reward through the Montgomery County Crime Solvers organization, for information that leads to the recovery of a laptop computer and external hard drive that contained personal information for millions of veterans.

Montgomery County Police are working with the FBI and the VA OIG in the investigation of this residential burglary that occurred on May 3, 2006, in the Aspen Hill community of Montgomery County, Maryland.

At this stage of the investigation there is no evidence that the suspect or suspects responsible for the theft had any knowledge of what information was stored on the hard drive. The primary objective of the investigation is the recovery of the laptop and external hard drive.

Anyone who can provide information that leads to the recovery of the laptop and external hard drive that contains the veterans’ data should call Crime Solvers of Montgomery County at 1-866-411-TIPS (8477). A cash reward of $50,000 will be paid for information provided to the Crime Solvers tip line that leads to the recovery of these items.

C2. How is information about this incident being shared?

We are providing as much information as we have about the incident and alerting veterans of the situation. We are in the process of identifying who may have been affected so we can provide them more information, where possible.

Veterans can go to www.FirstGov to get information on this matter.

C3. Will VA send me a letter?

The VA is working quickly to send individual notification letters to veterans to every extent possible. Due to the number of veterans who potentially could have been affected, VA is developing a method for individual notifications, where possible. We do not yet know when these letters will be released.

Letters will go out to all veterans for whom we are able to obtain an address, regardless of whether or not they are currently receiving VA benefits.

C3.a. When will more information be available?

VA will provide as much information as possible in a letter to affected veterans. We do not know the timeframe for release of these letters, but VA is working as fast as possible. In the meantime, continue to be vigilant. If you have access to the Internet, updated information will be provided at www.FirstGov.gov.

C4. What will be done to prevent this from happening in the future?

VA has safeguards in place for use and release of private information. VA provides ongoing privacy training to all employees and has directed all VA employees complete the cyber security and privacy awareness courses by June 30, 2006.